PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Raffaele, Eric ; et al.**	Examiner:	Gortayo, Dangelino N.
Serial No.:	**10/616,582**	Art Unit:	2168
Filed:	**July 9, 2003**	Our Ref:	50005197-3US B-4504DIV 621038
For:	"PROCESS FOR EXECUTING A DOWNLOADABLE SERVICE RECEIVING RESTRICTIVE ACCESS RIGHTS TO AT LEAST ONE PROFILE FILE"	Date:	January 5, 2009
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Commissioner for Patents

Sir:

This is an appeal from the latest rejection for the above identified patent application. Please deduct the fee set forth in 37 C.F.R. 41.20(b)(2) for submitting this Brief from deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston,

TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

JURISDICTION

The Board has jurisdiction under 35 U.S.C. 134(a). The Examiner mailed a final rejection on August 4, 2008, setting a three-month shortened statutory period for response. The time for responding to the final rejection expired on November 4, 2008. Rule 134. A notice of appeal was filed on November 4, 2008. The time for filing an appeal brief is two months after the filing of a notice of appeal. Bd.R. 41.37(c). The time for filing an appeal brief expires on January 5, 2009 (January 4 being a Sunday). The appeal brief is being filed on January 5, 2009.

TABLE OF CONTENTS

Pursuant to 37 C.F.R. Bd. R. 41.37(i), the present Appeal Brief contains the following items as required by 37 C.F.R. Bd. R. 41.37(e):

TABLE OF AUTHORITIES

Pursuant to 37 C.F.R. Bd. R. 41.37(j), the present Appeal Brief makes reference to the following court and administrative decisions (alphabetically arranged), statutes, and other authorities:

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Rejection of claims 1-3 and 16 as being anticipated under 35 U.S.C. 103(a) by U.S. Patent No. 7,206,844 to Gupta in view of U.S. Pat. No. 6,854,016 to Kraenzel et al.

Issue 2: Rejection of claim 12 as being unpatentable under 35 U.S.C. 103(a) over Gupta and Kraenzel and further in view of U.S. Publication 2001/0045451 to Tan.

STATEMENT OF FACTS

[0001] In rejecting claims 1–3 and 16, the Examiner cites Gupta (Abstract; col. 5 ll. 35-46; col. 5 l. 56 - col. 6 l. 27; col. 6 ll. 48-67; col. 7 ll. 1-8 and 16-28; col. 10 ll. 32-53; col. 10 l. 66 - col. 11 l. 11; col. 12 l. 45 - col. 13 l. 32; col. 13 ll. 15-25 and ll. 34-54; col. 16 ll. 9-19; col. 17 ll. 41 - col. 18 l. 13; col. 19 ll. 24-57; and col. 20 ll. 19-29) and Kraenzel (col. 12 l. 66 - col. 13 l. 35; col. 18 ll. 32-67).

[0002] The Examiner cites to col. 10 ll. 33-58 of Gupta, which discloses: "In an embodiment of the invention, communication link 322 between a client in client tier 302 and webtop server 308 uses both the Hypertext, Transmission Protocol (HTTP) and Remote Method Invocation (RMI). Similarly, communication link 324 between webtop server 308 and application server

310 uses both HTTP and RMI. In one or more embodiments of the invention, communication link 324 between webtop server 308 and application server 310 uses the Castanet product to transmit information (channels) from webtop server 308 to application server 310 and vice versa. Alternatively, instead of the Castanet product, an HTTP Distribution and Replication Protocol (DRP protocol) may be utilized. Using DRP, a client can download only the data (or application) that has changed since the last time the client checked (i.e., only the differences are downloaded). The DRP protocol uses content identifiers to automatically share resources that are requested more than once (thereby eliminating redundant transfers of commonly used resources). Additionally, the DRP protocol uses a data structure called an index that describes meta data (e.g., the exact state of a set of data files). The DRP protocol is more fully described in the document entitled "The HTTP Distribution and Replication Protocol" (1997) available at "http://www.w3.org/TR/NOTE-drp". It should be apparent, however, to one of ordinary skill in the art that other communication techniques and/or protocols can be used for communication links 322 and 324."

[0003] Gupta describes a method for distributing code resident on a remote application server to a local server, wherein a client machine (302) requests

an application program from a webtop server (308), the webtop server downloads the requested application from an application server (310) and stores the application, and allows the application (e.g. Java applets) to execute on the client machine. [col. 9 l. 65 - col. 11 l. 11, and Figure 3, elements 302, 308 and 310].

[0004] Gupta teaches that "The sandbox approach has clear disadvantages. An applet that is confined to its namespace cannot access information that is stored in a local file system. Further, confined applets cannot pool or share resources such as memory." [col. 5 ll. 8-31].

[0005] Gupta teaches that "Where the program software is written as Java applets, webtop server 308 becomes the applet-host once the applets are transferred from application server 310. Thus, when the applet is executed on the client, the applet can communicate back to webtop server 308 as the host of that applet thereby satisfying the sandbox security paradigm." [Gupta, col. 11 ll. 6-11].

[0006] Gupta teaches that "A service may, for example, process secure information and must therefore be executed in a secure environment such as application server 310. The service's proxy forwards the client's request to

the service that is running on application server 310." [Gupta, col. 17 ll. 43-45].

ARGUMENT

With respect to the rejection under §103, the claims stand or fall together.

Issue 1: Rejection of claims 1-3 and 16 as being anticipated under 35 U.S.C. 103(a) by U.S. Patent No. 7,206,844 to Gupta in view of U.S. Pat. No. 6,854,016 to Kraenzel et al.

In the Action of August 4, 2008, the Examiner continues to reject claims 1-3 and 16 stand rejected under 35 U.S.C. 103(a) as being anticipated by Gupta in view of Kraenzel et al. Appellants have previously explained that this is not correct because while the applet of Gupta executes on the client, it is controlled by (and stored on) a webtop server. [Amendment filed May 5, 2008, pages 4-5]. In particular, Appellants noted that in Gupta a client machine (302) requests an application program from a webtop server (308), the webtop server downloads the requested application from an application server (310) and stores the application, and allows the application (e.g. Java applets) to execute on the client machine. "Where the

program software is written as Java applets, webtop server 308 becomes the applet-host once the applets are transferred from application server 310. Thus, when the applet is executed on the client, the applet can communicate back to webtop server 308 as the host of that applet thereby satisfying the sandbox security paradigm." [Gupta, col. 11 ll. 6-11].

Thus, the applet of Gupta executes on the client, but is controlled by (and stored on) the webtop server. It is the webtop server that provides the equivalent of a confined runtime environment, not the client machine. Alternatively, such a confined runtime environment may be provided by the application server, but again not by or on the client machine: "A service may, for example, process secure information and must therefore be executed in a secure environment such as application server 310. The service's proxy forwards the client's request to the service that is running on application server 310." [Gupta, col. 17 ll. 43-45]. Regardless, it is clear that Gupta discloses a method that requires at least two, or sometimes three, separate computers to execute a process in a secure manner - which is not the same as or anticipatory of the claimed method for executing on a user's computer. Gupta makes it clear that his method is not a typical sandbox because "The sandbox approach has clear disadvantages…" [col. 5 ll. 8-31].

Presently the Examiner replies to the above by asserting that the claimed arranging a confined run time environment is "read to mean that a confined run time environment is set up and organized *by actions executed in the client computer*." [Office Action at p. 8 ¶3, emphasis added] Appellants respond with the following new counter-arguments that have not been previously presented to the Examiner. In particular, Appellants submit that the Examiner unequivocally acknowledges that this is not what Gupta teaches in the very same paragraph, wherein he admits that "As seen in the cited figures, the *webtop server and client work in a partnership* on one side to access application servers, and *the client* as cited *arranges for the webtop server to retrieve and store* program software from the application server, to be executed in a client." [emphasis added] Applicants thus submit that the Examiner in essence makes their point - that Gupta requires at least two machines (client and webtop server) to provide a confined run time environment - whereas the present invention provides such a confined run time environment solely on the user's computer. The Examiner only reinforces Appellants' argument on page 11 of the Action at line 2, wherein he unequivocally states that "the client sets up a confined runtime environment *in the webtop server*."

In their previous submission of May 2008, Appellants have also noted that there is nothing in Gupta that even mentions the opening of communications ports and sockets, and certainly not the claimed confined run time environment assigned a second communication port and socket. Presently the Examiner retorts that "as disclosed in column 10 lines 33-58, the link between a webtop server and the application server transfer data in specific channels of communications link, as determined by different protocols. Therefore, Gupta teaches assigning a second communication port and socket." Appellants submit, with all due respect, that this is neither correct nor logical.

In particular, Appellants respond with the following new counter-arguments that have not been previously presented to the Examiner. Appellants submit that the cited passage of Gupta does not in fact even allude to transferring data "in specific channels" - it merely provides a laundry list of the different communication protocols that may be utilized, and only mentions "channels" as a *synonym for "information."* [Gupta, col. 10 l. 40]. Furthermore, even if Gupta did assign specific channels for different protocols, there is still no logical inference to be drawn from this

regarding the opening of a second socket and port for the confined run time environment that is *shared* between the webtop server and the client.

Appellants have further noted in their previous submission of May 2008 that Gupta also teaches nothing that would lead one to understand that the webtop server has restricted access to the user's profile. Presently the Examiner counters by noting that Gupta teaches tracking a client session with a cookie created by an applet downloaded to the client machine, which cookie also determines which applications and network services the client is allowed to access, and concludes that "Therefore, Gupta in view of Kraenzel teaches restricted access to the user's profile." Appellants respond with the following new counter-arguments that have not been previously presented to the Examiner. Specifically, Appellants respectfully submit that the Examiner's conclusion finds absolutely no support in nor connection to his explanation. Giving the client access to the network bears no relation whatsoever to giving an application access to the client profile. This is not just common knowledge in the art - it is common sense.

To maintain a complete record, Appellants further note for the first time, in a counter-argument that has not been previously presented to the Examiner, that the Examiner's statement on p. 10, ll. 8-11, ("The security

features of the system is further disclosed in column 20 lines 19-34, wherein an applet is determined to be trusted or untrusted, and it is determined how much access an application being executed on a webtop server has to computer resources.") is equally irrelevant. A client profile is not the same as the computer resources - this is at least common knowledge in the art. Furthermore, the Examiner once again reinforces Appellants' previous point, by once more admitting that the application is being executed on the *webtop server*.

In their previous submission of May 2008 Appellants also disagreed with the Examiner's contention that Gupta teaches the claimed "executing said service within said confined run time environment whereby said service is given restricted access to said at least one profile file" because the webtop server of Gupta does not install application software, and it does not pass data onto to the client machine. The webtop server *stores* the application software, and *passes the software* to the client for execution thereon. Furthermore, and very importantly, there is no teaching that the application programs that the webtop server allows to execute on the client machines have access to the user profiles that are stored on the webtop server. Gupta is very explicit that it is only local services that execute on the webtop server itself that have access to the user profiles stored on the webtop

server - such as for instance login service 514C. There is absolutely no mention by Gupta of allowing an application executing on a client machine to access a user profile stored on a webtop server.

Presently the Examiner replies that "Gupta … teaches that the webtop server stores and caches application data that a client utilizes, the client fetching application applets that is executed for the web service…[T]he client sets up a confined runtime environment in the webtop server, which is in contact with application servers containing application data… [T]he application software that is determined to be safe in a webtop server is then downloaded to the client to be executed. Therefore, Gupta teaches executing said service within said confined run time environment whereby said service is given restricted access to said at least one profile file." Appellants respond with the following new counter-arguments that have not been previously presented to the Examiner. Specifically, Appellants once again respectfully submit that the Examiner's conclusion bears absolutely no logical connection to the supporting explanation. The client profile is not even mentioned by the Examiner in his explanation, which does in fact play no role in checking the status of software or downloading it onto the client machine. Furthermore, there is absolutely nothing in Gupta - and, for that matter, in the Examiner's explanation - that mentions affording *restricted access* to such a

profile; of course, this is entirely congruous with the lack of a mention of a *profile* in the first place.

Finally, Applicants respectfully disagree with the Examiner's allegation that the skilled person would find it obvious to attempt to combine Gupta and Kraenzel. The Examiner supports his finding of obviousness by averring that "motivation can be found in the prior art of Kraenzel … wherein permission and authorization is utilized for code and applets downloaded online, as the user profile found in the clients of Kraenzel is applied to the applet distribution system of Gupta. As further stated in Gupta… there is a need to ensure that code downloaded from another source does not corrupt the client, and security measures are needed." Appellants respond with the following new counter-arguments that have not been previously presented to the Examiner. In particular, Appellants yet again respectfully submit that there is no connection between these two goals - how exactly is the skilled person to "apply" the user profile of Kraenzel to the applet distribution system of Gupta, and how would such a user profile "ensure that code downloaded from another source does not corrupt the client"? What connection is there between a user profile and "security measures [that] are needed"? Appellants submit that the Examiner's proffered motivation is not based upon a reasonable inference, as the skilled person looking to practice the system of Gupta would feel no need for or

benefit from attempting to force-fit a user profile such as taught by Kraenzel therein.

Appellants further respectfully submit, in the following new counter-arguments that have not been previously presented to the Examiner, that the Examiner's conclusion of obviousness falls short of the requirements for a proper 35 USC §103 rejection as set forth in the new *KSR v. Teleflex* Examination Guidelines of October 10, 2007.

The new Guidelines provide that "When making an obviousness rejection, Office personnel must therefore ensure that the written record includes findings of fact concerning the state of the art and the teachings of the references applied. In certain circumstances, it may also be important to include explicit findings as to how a person of ordinary skill would have understood prior art teachings, or what a person of ordinary skill would have known or could have done. Factual findings made by Office personnel are the necessary underpinnings to establish obviousness." There are no such factual findings in the present Action, rather in their stead conclusory statements as to what the skilled person, according to the Examiner's unexplained opinion, would allegedly have done.

The Guidelines further admonish that "Although a rejection need not be based on a teaching or suggestion to combine, a preferred search will be directed to

finding references that provide such a teaching or suggestion if they exist." As explained immediately above, the alleged suggestion advanced by the Examiner bears in fact no relation to the actual teachings of the prior art.

The Guidelines further set forth that "Any obviousness rejection should include, either explicitly or implicitly in view of the prior art applied, an indication of the level of ordinary skill." No such indication, explicit or implicit, is to be found in the Action.

Perhaps the most instructive portion of the Guidelines is the clear statement that "The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Court quoting *In re Kahn* stated that " '[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.' " Again, rather than offer articulated reasoning with some rational underpinning, the Examiner merely throws together the disparate goals of Gupta and Kraenzel into the same sentence and thereby declares obviousness.

These Guidelines do make clear that "the familiar teaching-suggestion-

motivation (TSM) rationale" can still be employed by Examiners in making an obviousness rejection. However, as noted above, the motivation asserted by the Examiner does not in fact exist and furthermore the Examiner has not even mentioned where a suggestion is allegedly to be found in either of the cited references.

In view of the above, Appellants submit that Gupta and Kraenzel and the presently claimed inventions are patentably distinct and respectfully request the Board to kindly overturn the Examiner on appeal and withdraw the rejection of claims 1 and 16.

Claims 2 and 3 depend from claim 1. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claim 1, Appellants submit that claims 2 and 3 are also allowable at least by virtue of their dependencies.

Issue 2: Rejection of claim 12 as being unpatentable under 35 U.S.C. 103(a) over Gupta and Kraenzel and further in view of U.S. Publication 2001/0045451 to Tan.

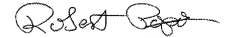
In the final Action of August 4, 2008, the Examiner continues to reject claim 12 as being unpatentable under 35 U.S.C. 103(a) over Gupta and Kraenzel and

further in view of Tan. Appellants note that claim 12 depends from claim 1, and thus submit that claim 12 is allowable at least by virtue of its dependency from claim 1.

CONCLUSION

For the extensive reasons advanced above, Appellants respectfully contend that each claim is patentable. Therefore, reversal of all rejections and objections and re-opening of the prosecution is respectfully solicited.

Respectfully submitted,



Robert Popa
Attorney for Appellants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@la.ladas.com

CLAIMS APPENDIX

Claim 1. A process for executing a downloadable service with specific access rights to at least one profile file in a user's computer, said computer comprising a web browser communication to an internet or intranet via a first communication port and socket, said process comprising:

arranging a confined run time environment which is assigned a second communication port and socket and provided with restricted access to at least one profile file that is located on the user's computer;

downloading said service through said second communication port so that it is received by said confined run time environment; and

executing said service within said confined run time environment whereby said service is given restricted access to said at least one profile file.

2. (original) The process according to claim 1 wherein said confined run time environment is an extended sandbox having restrictive access to said at least one profile file.

3. (previously presented) The process according to claim 2 wherein the service is

downloaded under the form of a set of java code containing classes structure packaged within a signed archive file; the service comprising remote Internet data, a list of requested data that are needed to personalise the service, and code to sort remote internet data using request accessible data.

12. (previously presented) The process according to claim 1 wherein said downloadable service is an authentication service cooperating with a master card.

16. (previously presented) A process for executing a downloadable service with specific access rights to at least one profile file in a user's computer, said computer comprising a web browser communication to the internet or intranet via a first communication port and socket, said process comprising:

arranging a confined run time environment in said user's computer, said confined run time environment being assigned a second communication port and socket and provided with restricted access to at least one profile file that is located on the user's computer;

downloading said service through said second communication port so that it is received by said confined run time environment; and

executing said service within said confined run time environment whereby said service is given restricted access to said at least one profile file.

CLAIMS SUPPORT AND DRAWING ANALYSIS APPENDIX

MEANS OR STEP PLUS FUNCTION ANALYSIS APPENDIX

Claim 1. A process for executing a downloadable service with specific access rights to at least one profile file in a user's computer **{element 1 in Fig. 1; p. 4 ll. 13-15}**, said computer comprising a web browser **{element 15 in Fig. 1}** communication to an internet or intranet **{element 2 in Fig. 1; p. 8 ll. 1-12}** via a first communication port and socket **{p. 4 ll. 14-15; p. 11 ll. 1-4}**, said process comprising:

arranging a confined run time environment **{element 11 in Fig. 1; p. 11 ll. 1-2 and 8-9}** which is assigned a second communication port and socket **{p. 11 ll. 1-4}** and provided with restricted access to at least one profile file **{element 14 in Fig. 1; p. 8 ll. 26-27 and p. 12 ll. 9-10}** that is located on the user's computer **{p. 9 l. 1 - p. 10 l. 5}**;

downloading **{steps 23-25 in Fig. 2}** said service through said second communication port so that it is received by said confined run time environment **{p. 10 l. 33 - p. 11 l. 31}**; and

executing **{step 28 in Fig. 2}** said service within said confined run time environment whereby said service is given restricted access to said at least one profile file **{p. 12 ll. 14-16}**.

Claim 16. A process for executing a downloadable service with specific access rights to at least one profile file in a user's computer **{element 1 in Fig. 1; p. 4 ll. 13-15}**, said computer comprising a web browser **{element 15 in Fig. 1}** communication to the internet or intranet **{element 2 in Fig. 1; p. 8 ll. 1-12}** via a first communication port and socket **{p. 4 ll. 14-15; p. 11 ll. 1-4}**, said process comprising:

arranging a confined run time environment **{element 11 in Fig. 1; p. 11 ll. 1-2 and 8-9}** in said user's computer, said confined run time environment being assigned a second communication port and socket **{p. 11 ll. 1-4}** and provided with restricted access to at least one profile file **{element 14 in Fig. 1; p. 8 ll. 26-27 and p. 12 ll. 9-10}** that is located on the user's computer **{p. 9 l. 1 - p. 10 l. 5}**;

downloading **{steps 23-25 in Fig. 2}** said service through said second communication port so that it is received by said confined run time environment **{p. 10 l. 33 - p. 11 l. 31}**; and

executing **{step 28 in Fig. 2}** said service within said confined run time environment whereby said service is given restricted access to said at least one profile file **{p. 12 ll. 14-16}**.

EVIDENCE APPENDIX

There is no evidence submitted with the present Brief on Appeal.

RELATED PROCEEDINGS APPENDIX

There are no other appeals or interferences related to the present application.